Analysis of Quantum Safe cryptography tools

Autor

Julio César Ruiz Gómez

Universidad de los Andes

Asesora

Nicolás Cardozo, PH.D.

Universidad de los Andes

Tesis

Departamento de ingeniería de sistemas y computación

Facultado de ingeniería

Universidad de los Andes

Bogotá D.C., Colombia

Agosto de 2024

1. Introducción

En los últimos años, la criptografía ha desempeñado un papel crucial en la protección de la información en diversos ámbitos, desde la comunicación personal hasta la seguridad nacional y las transacciones financieras. Los algoritmos criptográficos actuales, como RSA y ECC (Criptografía de curva elíptica), se basan en problemas matemáticos que son computacionalmente difíciles de resolver con la computación tradicional. Sin embargo, con el avance acelerado en el campo de la computación cuántica, la seguridad de estos algoritmos se ve seriamente amenazada.

La criptografía post-cuántica emerge como una respuesta a este desafío inminente. A diferencia de la criptografía tradicional, los algoritmos post-cuánticos están diseñados para ser resistentes a los ataques que podrían realizarse utilizando computadoras cuánticas. La computación cuántica, mediante algoritmos como el de Shor, tiene el potencial de descomponer números primos y resolver el logaritmo discreto de manera exponencialmente más rápida que las computadoras tradicionales, comprometiendo así la seguridad de los sistemas actuales.

El objetivo principal de esta tesis es evaluar la usabilidad y viabilidad de los algoritmos de cifrado post-cuánticos en la práctica. Esto incluye un análisis detallado de las principales familias de algoritmos post-cuánticos, como los basados en latices, LWE (learning with errors), ecuaciones cuadráticas y funciones hash. Se explorará su desempeño en términos de seguridad, eficiencia y aplicabilidad en diversos escenarios del mundo real.

1. Estado del arte en criptografía post-cuántica

La criptografía post-cuántica ha captado la atención de importantes instituciones y empresas debido a la inminente amenaza que representa la computación cuántica para la criptografía clásica. Organizaciones como NIST, Microsoft, Linux Foundation, IBM e Intel juegan un papel crucial en este ámbito.

El NIST (Instituto Nacional de Estándares y Tecnología) lidera los esfuerzos de estandarización de algoritmos post-cuánticos a través de su proyecto de estandarización, recientemente ha seleccionado los primeros cuatro algoritmos que serán estandarizados. Su papel es fundamental para establecer directrices y asegurar que las nuevas tecnologías criptográficas sean adoptadas a nivel global.

Microsoft ha estado invirtiendo significativamente en investigación y desarrollo de algoritmos post-cuánticos. Su contribución se centra en asegurar que sus infraestructuras de software y servicios en la nube sean resistentes a las amenazas de la computación cuánticas. Microsoft también es miembro activo de alianzas y colaboraciones que promueven la criptografía post-cuántica.

IBM, por su parte, ha desarrollado un plan de migración hacia la criptografía post-cuántica para ayudar a las agencias federales y empresas a prepararse para la transición. IBM también colabora estrechamente con organismos de estandarización para asegurar que sus soluciones tecnológicas sean robustas frente a las amenazas cuánticas.

Intel está involucrada en la investigación y desarrollo de tecnologías de seguridad post-cuántica, trabajando en la integración de estas tecnologías en sus procesadores y hardware de seguridad. Intel también participa en iniciativas colaborativas para asegurar que sus productos mantengan la seguridad frente a futuros avances en la computación cuántica.

La Post-Quantum Cryptography Alliance (PQCA), una coalición de empresas y organizaciones desempeña un papel crucial en la promoción de soluciones de criptografía post-cuántica. La PQCA se enfoca en desarrollar software de código abierto que aborda los desafíos de seguridad planteados por la computación cuántica, promoviendo la adopción de criptografía resistente a esta tecnología emergente.

Estas instituciones y empresas no solo están en la vanguardia de la investigación y desarrollo de tecnologías post-cuánticas, sino que también colaboran estrechamente para garantizar una transición segura y eficiente hacia un futuro donde la seguridad criptográfica pueda resistir los avances de la computación cuántica. Su trabajo conjunto es esencial para proteger la infraestructura digital global y asegurar que las futuras generaciones de tecnología sean seguras y confiables.

1. Algoritmos escogidos

En la siguiente tabla se recogen los algoritmos de criptografía post-cuántica más relevantes según el NIST y los que fueron desarrollados o apoyados por empresas reconocidas como Microsoft.



1. Descripción de los algoritmos

Algunos algoritmos en la tabla se consideran "primary standard" debido a que son los más maduros, eficientes y versátiles. Estos algoritmos, designados por el NIST, incluyen Classic McEliece, CRYSTALS-KYBER, NTRU, SABER, CRYSTALS-DILITHIUM, FALCON y Rainbow. Por otro lado, existen algoritmos denominados "alternate candidates" que, aunque no alcanzan el mismo grado de madurez que los "primary standard", son seguros y se estandarizan para asegurar diversidad criptográfica, especialización en aplicaciones con características específicas y redundancia en caso de que se descubran vulnerabilidades en otros algoritmos. Estos algoritmos alternativos son FrodoKEM, Picnic y SIKE.

Finalmente, el algoritmo de qTESLA fue retirado durante la 3ª ronda del proceso de estandarización ya que se encontraron problemas de seguridad, el desempeño no era competitivo con respecto a las alternativas y no tenía la madurez suficiente para avanzar a la siguiente ronda.

1. Criterios de evaluación

Los algoritmos previamente mencionados fueron escogidos teniendo en cuenta varios aspectos.

Diversidad Criptográfica: Estos algoritmos abarcan una amplia variedad de enfoques criptográficos, incluyendo criptografía de códigos (Classic McEliece), latices (CRYSTALS-KYBER, NTRU, SABER, FrodoKEM), funciones hash (Picnic), curvas elípticas isogénicas (SIKE), firmas basadas en esquemas multivariados (Rainbow), y más. Esta diversidad es crucial para proporcionar una visión completa de las técnicas y enfoques en criptografía post-cuántica.

Evaluación y Reconocimiento por el NIST: Todos estos algoritmos han sido considerados seriamente por el Instituto Nacional de Estándares y Tecnología (NIST) en su proceso de estandarización de criptografía post-cuántica. Algunos de ellos han sido designados como "primary standards" debido a su madurez, eficiencia y versatilidad, mientras que otros son "alternate candidates", reconocidos por su seguridad y especialización en aplicaciones específicas.

Seguridad y Resiliencia: Estos algoritmos han demostrado ser resistentes a los ataques tanto clásicos como cuánticos, cumpliendo con los estrictos criterios de seguridad necesarios para la criptografía en la era post-cuántica. La inclusión de algoritmos que han pasado múltiples rondas de evaluación asegura que las soluciones propuestas son robustas y confiables.

Rendimiento y Eficiencia: La selección incluye algoritmos que han demostrado un rendimiento competitivo y una implementación eficiente en términos de velocidad, consumo de recursos y escalabilidad. Esto es esencial para asegurar que las soluciones criptográficas puedan ser aplicadas en una variedad de entornos prácticos.

La computación cuántica representa una amenaza directa para muchos de los algoritmos criptográficos tradicionales, especialmente aquellos basados en problemas de factorización y logaritmos discretos, como RSA y ECC. En consecuencia, la exploración de alternativas resistentes a la computación cuántica ha llevado al desarrollo de varias familias de algoritmos post-cuánticos, tales como KEMs (Mecanismos de Encapsulamiento de Claves), firmas digitales y esquemas de cifrado basados en diferentes problemas matemáticos. Comparar estos algoritmos entre sí y con los tradicionales permitirá ofrecer a los usuarios una guía para seleccionar el más adecuado en función de sus criterios específicos de uso, como la seguridad, la eficiencia en tiempo, la eficiencia espacial, y la compatibilidad. Este proyecto pretender proporcionar una base técnica para los profesionales en seguridad, ofreciendo una guía clara y práctica para la selección de algoritmos en diferentes escenarios de uso.

**Justificación**

Este proyecto permitirá comparar las diferentes familias de algoritmos post-cuánticos con algoritmos tradicionales proporcionando una base de conocimiento para una transición hacia un entorno resistente a la computación cuántica, y así, brindar seguridad con enfoque a la viabilidad de su uso.

Los criterios de evaluación permitirán a los usuarios seleccionar algoritmos según varias métricas tales como tiempos de ejecución, consumo de memoria, o compatibilidad en el entorno objetivo.

Este proyecto plantea una metodología estructurada que permitirá evaluar y comparar cada algoritmo de manera objetiva y así ayudar a desarrolladores y empresas a escoger el mejor según sus requerimientos específicos y escenarios de uso.

**Criterios de evaluación**

Rendimiento en tiempo (latencia y rendimiento)

La eficiencia temporal es crucial para aplicaciones que requieren alta velocidad o tiempos de respuesta rápidos, como las transacciones en tiempo real, autenticación en línea, o servicios en la nube.

En aplicaciones bancarias, una latencia elevada puede causar demoras en las transacciones, impactando la experiencia del usuario. En redes de IoT, la capacidad de realizar operaciones criptográficas rápidamente puede significar una mejor respuesta del sistema en casos críticos, como en vehículos autónomos o equipos de telemedicina. Comparar tiempos de ejecución, como generación de claves y verificación, permite identificar algoritmos que cumplen con las demandas de estos entornos.

**Eficiencia espacial**

Los algoritmos post-cuánticos suelen tener claves y artefactos más grandes que los algoritmos clásicos, lo cual impacta significativamente el uso de memoria y ancho de banda. Evaluar la eficiencia espacial ayuda a determinar si un algoritmo es viable en sistemas con limitaciones de almacenamiento o donde el tráfico de datos es costoso.

En dispositivos IoT y sistemas embebidos, donde la memoria es limitada, el tamaño de las claves y firmas puede definir si un algoritmo es utilizable o no. En sistemas de comunicación remotos o redes con ancho de banda limitado, como satélites o sensores rurales, el tamaño de los artefactos criptográficos impacta directamente los costos y la velocidad de transmisión.

**Consumo de recursos (CPU y memoria)**

La eficiencia en el uso de recursos permite que los algoritmos puedan ser ejecutados en dispositivos con hardware limitado sin comprometer el rendimiento de otras funciones críticas.

En dispositivos móviles, sistemas embebidos, y redes IoT, el consumo de CPU y memoria es clave, pues un algoritmo que exige demasiados recursos puede drenar la batería rápidamente o hacer el sistema inestable. En servidores y centros de datos, la capacidad de realizar cifrados de manera eficiente permite soportar un mayor volumen de usuarios y reducir costos operativos.

**Descripción de algoritmos**

Redes Lattice: Esta familia se basa en problemas geométricos relacionados con retículos o redes en espacios multidimensionales. Los problemas de redes, como el problema del vector más corto (SVP) y el problema de aprendizaje con errores (LWE), son difíciles de resolver incluso para computadoras cuánticas. El algoritmo Kyber de tipo KEM (Key Encapsulation Mechanism) proporciona encriptación de clave pública basado en redes. Es uno de los algoritmos seleccionados por el NIST para estandarización.

Codificación de Error: Estos algoritmos se basan en problemas de teoría de códigos, como la corrección de errores. La idea es construir sistemas criptográficos resistentes a ataques cuánticos aprovechando la dificultad de decodificar sin la clave correcta. BIKE (Bit Flipping Key Encapsulation) es un algoritmo que usa problemas de corrección de errores en su diseño de cifrado y encapsulación de claves.

Isogenias de Curvas Elípticas: Estos algoritmos dependen de problemas complejos de matemáticas algebraicas relacionados con las isogenias entre curvas elípticas, difíciles de resolver incluso con computación cuántica. SIKE (Supersingular Isogeny Key Encapsulation) usa isogenias de curvas elípticas supersingulares para encapsulación de claves. Aunque SIKE fue considerado durante un tiempo, fue vulnerado en algunos aspectos y actualmente sigue en desarrollo y pruebas adicionales.

Hash: Los algoritmos de esta familia confían en la dificultad de encontrar colisiones en funciones hash, algo extremadamente difícil de resolver con computadoras cuánticas. El algoritmo de firmas SPHINCS+ está basado únicamente en funciones hash, lo que lo hace resistente a ataques cuánticos sin depender de suposiciones algebraicas complejas. Fue seleccionado por el NIST para estandarización.

Multivariable: Los algoritmos de esta familia usan sistemas de ecuaciones multivariables no lineales, que son difíciles de resolver para computadoras cuánticas debido a su complejidad. Rainbow es un esquema de firma digital basado en sistemas multivariables de ecuaciones cuadráticas, que proporciona alta seguridad. También fue uno de los algoritmos en consideración para la estandarización.

**Proceso de selección de algoritmos**

Estos algoritmos fueron selccionados por su equilibrio en criterios de seguridad, velocidad y variedad matemática para cubrir diferentes necesidades criptográficas. Al seleccionar Kyber, SIKE, BIKE, Rainbow y SPHINCS+, se abordan varias de estas necesidades, cada uno con fortalezas únicas.

Kyber es ideal para sistemas donde se necesitan operaciones rápidas y seguras de encapsulación de clave. También tiene un rendimiento excelente, incluso en dispositivos de baja capacidad.

SIKE, si bien se descubrieron vulnerabilidades, aún está en desarrollo y ofrece un enfoque interesante en curvas elípticas supersingulares. En comparación con otros algoritmos, SIKE es menos rápido, pero su ventaja radica en el tamaño reducido de claves, lo que beneficia a aplicaciones con limitaciones de espacio.

BIKE es una excelente opción para encapsulación de claves en aplicaciones donde la eficiencia y seguridad son importantes, además de diversificar el conjunto al ser un algoritmo de codificación de error.

Rainbow es rápido en la generación de firmas y tiene un tamaño de clave adecuado para muchas aplicaciones.

SPHINCS+ es una excelente opción para firmas digitales en escenarios donde la seguridad y la integridad de los datos son críticas, complementando la diversidad matemática del conjunto con su enfoque hash.

Para utilizar estos algoritmos se exploraron varias opciones como bouncy castle, crystals y liboqs. La primera opción descartada fue crystals ya que solo ofrecía el uso de Kyber y Dilithium. Por otro lado, bouncy castle y liboqs ofrecían los algoritmos utlizados en este proyecto junto con unos cuantos más. Sin embargo, por temas de compatibilidad con la versión de java usada se decidió finalmente usar liboqs por su amplio catálogo de algoritmos, simpleza a la hora de su uso y trayectoria como uno de los mejores proyectos de criptografía post-cuántica en java.